PRV

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

Intyg
Certificate

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

(71) *Sökande* / *Applicant (s)* — *Telefonaktiebolaget LM Ericsson, Stockholm SE*

(21) *Patentansökningsnummer* / *Patent application number* — *0202451-1*

(86) *Ingivningsdatum* / *Date of filing* — *2002-08-15*

Stockholm, 2003-01-08

För Patent- och registreringsverket
For the Patent- and Registration Office

Sonia André

Avgift
Fee

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

PATENT- OCH REGISTRERINGSVERKET
SWEDEN

Postadress/Adress
Box 5055
S-102 42 STOCKHOLM

Telefon/Phone
+46 8 782 25 00
Vx 08-782 25 00

Telex
17978
PATOREG S

Telefax
+46 8 666 02 86
08-666 02 86

FLEXIBLE SIM-BASED DRM AGENT AND ARCHITECTURE

TECHNICAL FIELD OF THE INVENTION

The present invention relates to digital rights management (DRM) for managing digital content ordered and distributed over networks such as the Internet.

BACKGROUND OF THE INVENTION

The distribution of digital content or media data using modern digital communication technologies is constantly growing, increasingly replacing more traditional distribution methods. In particular, there is an increasing trend of downloading or streaming digital content from a content provider to a user, which then typically renders or executes the content using a rendering or executing device according to some usage rights or rules specified in a license associated with the digital content. Due to the advantages of this form of content distribution, including being inexpensive, fast and easy to perform, applications can now be found for distribution of all types of media such as audio, video, images, electronic books and software.

However, with this new way of distributing digital media content comes the need for protecting the content provider's digital assets against unauthorized usage and illegal copying. Copyright holders and creators of digital content naturally have a strong economic interest of protecting their rights, and this has lead to an increasing demand for digital rights management (DRM). DRM is generally a technology for protecting the content provider's assets in a digital content distribution system, including protecting, monitoring and restricting the usage of the digital content as well as handling payment. A DRM system thus normally includes components for encryption, authentication, key management, usage rule management and charging.

The most basic threats to a DRM system include eavesdropping, illegal copying, modification of usage rules, and repudiation of order or delivery of content. Most of these basic security problems are solved by standard cryptographic techniques, including encryption, authentication and key management. However, what basically distinguishes the security problems of a DRM system from other general security problems is that not even the other end-part of the communication (the end user) is completely trusted. In fact, the end-user might want to try to fraudulently extend his usage rights, for example rendering the media content more times than he has paid for or illegally copying the digital content to another rendering or executing device. Therefore, some form of rule-enforcement is required in the user's rendering or executing device. To this end, a tamper-resistant circuit and some formal language, such as XrML, expressing the usage rules are commonly used together with the basic cryptographic techniques mentioned above.

Unfortunately, it now and then happens that the algorithms in the tamper-resistant DRM circuits are hacked, and a piece of software that successfully cracks some vital part of the DRM security of a particular type of rendering device is openly distributed. From the viewpoint of the content provider, this makes all the rendering devices of this type unsecure for DRM purposes, and the content provider may have to stop providing digital content intended for these rendering devices, and instead use another algorithm that has not yet been hacked. Recalling and replacing all the concerned rendering devices is obviously very expensive for the manufacturer/content provider.

A robust DRM system will make copyright holders more willing to distribute their material and offer a wider selection of content for end users over open, untrusted channels such as the Internet. It will also provide business opportunities for network operators to provide the infrastructure for distribution, charging mechanism and so forth.

Another problem is that it is often difficult, sometimes even impossible, to move media content from one rendering or executing device to another. The media usage license is often associated with a single device, and if the user wants to use the content in another device, he needs a new license. This is a cumbersome procedure for the end-user, and reduces the flexibility in the user's media system.

SUMMARY OF THE INVENTION

The present invention overcomes these and other drawbacks of the prior art arrangements.

It is a general object of the present invention to provide a robust DRM system.

It is another important object of the invention to provide a very flexible and relatively secure client solution for digital rights management (DRM).

Yet another object of the invention is to provide a DRM method allowing the network operator to be more active in establishing and maintaining DRM functionality.

These and other objects are met by the invention as defined by the accompanying patent claims.

The basic idea according to the invention is to implement a DRM agent into a network subscriber identity module intended for cooperation with a client module capable of receiving digital content. The DRM agent generally includes DRM functionality for enabling usage, such as rendering or execution, of (encrypted) digital content provided to the client from a content provider.

In general, the DRM agent includes functionality for cryptographic processing of DRM metadata associated with the digital content to be rendered or executed. This metadata

may for example be an encryption/decryption key as well as the encrypted digital content itself. Normally, the DRM agent includes some basic functionality for more or less directly generating or extracting a decryption key to be used for decrypting the encrypted digital content. It is also possible to integrate the actual decryption of the digital content into the DRM agent, as well as functionality for rule-enforcement.

The network subscriber identity module is not limited to the standard SIM cards used in GSM (Global System for Mobile Communications) mobile telephones but can be any network subscriber identity module known to the art, including also UMTS (Universal Mobile Telecommunications System) SIM, WAP (Wireless Application Protocol) SIM and ISIM (Internet Multimedia Services Identity Module) modules. It is especially noted that the invention fits well into the emerging WAP-DRM standard.

Although the invention is particularly suitable for mobile units and mobile DRM, the invention is not limited to mobile phones and communicators. The invention can be used with any client module, including conventional PC systems.

In most standardized SIM modules, the DRM agent may interface authentication and keying algorithms pre-existing on the SIM, reusing the subscriber-operator relation manifested by the shared subscription key. The subscriber-operator relation may also be used for charging in the overall DRM system.

It has been recognized that it is particularly advantageous to implement the DRM agent as an application in the application environment provided by the network subscriber identity module's application toolkit. The DRM application agent can be preprogrammed into the toolkit application environment, or securely (preferably authenticated and encrypted) downloaded from a network operator associated with the subscriber identity module. The toolkit application environment is not the same as a true tamper resistant circuit, but it is far more secure than performing the DRM processing in a hostile PC (personal computer) environment, and more flexible than using hard-wired tamper

resistant circuits. For example, if a security flaw is found or if the whole DRM agent is hacked, the functionality is easily replaced or upgraded (even or the air interface) by a new DRM agent. It should be understood that although a software agent is particularly beneficial, it is also possible to have the DRM agent premanufactured as hardware in the network subscriber identity module.

The proposed solution provides increased flexibility for the end-user as well as the content provider and/or network operator. The network subscriber identity module is easily replaceable (even remotely upgradeable), "portable" between different rendering or executing devices as well as relatively secure.

Another interesting functionality suitable for implementation in the DRM agent is certification and registration of rendering or executing devices in the network subscriber identity module, preferably including functionality for ensuring secure transfer of the content-decryption key between the DRM agent and the actual rendering or executing device (assuming that the content-decryption takes place in the rendering device). Certification and registration is particularly important when the subscriber identity module is moved between different rendering or executing devices, or when using stand-alone rendering or executing equipment.

It is also beneficial to have the network operator (in processing a media order) and/or a content provider (in processing a request for content) authenticate that the network subscriber identity module used with the client includes a compliant DRM agent.

The invention offers the following advantages:

- From the end-user point of view, the invention provides flexible and upgradeable implementation of DRM agents, as well as "portability" between different rendering or executing devices.

- A manufacturer of rendering or executing devices (players) can easily configure players to run with an external DRM agent.
- A network operator can efficiently manage and upgrade DRM agents connected to the network, and the invention also opens up new business possibilities for the operator acting as a trusted center for content distribution.

Other advantages offered by the present invention will be appreciated upon reading of the below description of the embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention, together with further objects and advantages thereof, will be best understood by reference to the following description taken together with the accompanying drawings, in which:

Fig. 1 is an overview of a digital rights management system for ordering digital content over a network illustrating the relevant parties and their mutual relationships;

Fig. 2A schematically illustrates a client module according a preferred embodiment of the present invention;

Fig. 2B schematically illustrates a subcriber identity module according a preferred embodiment of the present invention;

Fig. 3 is a flow diagram illustrating a digital rights management method according to a preferred embodiment of the invention;

Fig. 4 is a schematic diagram illustrating an example of client-operator authentication key agreement client-side digital rights management, as well as the associated client-operator communication;

Fig. 5 illustrates a subscriber identity module and an associated rendering device according to an embodiment of the invention;

Fig. 6 illustrates a subscriber identity module and an associated rendering device according to another embodiment of the invention;

Fig. 7 illustrates a subscriber identity module and an associated rendering device according to yet another embodiment of the invention;

Fig. 8 is a schematic diagram of an example of a DRM protocol involving an operator, a SIM, a content provider and a rendering device; and

Fig. 9 is a schematic block diagram of relevant parts of a DRM system operating based on the protocol of Fig. 8.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

The present invention is generally applicable to digital rights management (DRM) used in a digital content ordering and distribution system. In such ordering and distribution system, digital content or media is provided from a content provider to a client over a network, e.g. Internet or a wireless network for mobile communication, managed by a network operator. In order to facilitate understanding of the invention, a brief discussion of the general DRM functions follows. As was mentioned in the background section, DRM is used for protecting the copyright holders' assets in a digital content ordering and distribution system. In this system, DRM typically regards authentication and key management, usage rights management and charging. These DRM functions are implemented in DRM modules arranged in the relevant parties, i.e. for example in a client module, in a server of the network operator and in a media or content server of the content provider.

Starting with authentication and key management, authentication is used to identify the parties in the digital content ordering and distribution process. Techniques well known in the art, such as message authentication and digital signatures using cryptographic keys [1], may be employed for authentication. In addition, techniques for marking or stamping digital content, so that it can be tracked during the delivery process and subsequent usage, may be used. Watermarking and fingerprinting are two techniques that usually are employed for content marking. The DRM modules in the system also transport, store and generate, in a secure way, cryptographic keys for use in the digital content ordering and distribution process. The keys are employed for cryptographically protecting messages, including the actual digital content, during the delivery over the network.

The DRM modules also perform usage rule management, including rule-enforcement. The ordered digital content is associated with a license or digital permit specifying the client's usage rules and rights of the obtained digital media. This form of management is about the digital content itself and deals with issues such as, who gets it, how is it delivered, how may it be used, how many times may it be used (rendered, executed, saved, forwarded, copied and or modified), how long does the rights last, who gets paid, how much they get paid and how. Some or all of these issues are specified in the license, which may be delivered together with the digital content. In order to describe the usage rules, special languages called rights languages have been developed. Two of the most prevalent rights languages used today are Rights Markup Language (XrML) and Open Digital Rights Language (ODRL). In the client's rendering or executing device, the DRM module is implemented to ensure that the usage, most often rendering, follows what is described in the usage rules and to prevent repudiation of the digital content.

Finally, charging management generally refers to the procedure of the actual payment for usage of the digital content. Several different techniques are used, such as credit card techniques for payment over Internet or payment through a subscription.

A digital content ordering and distribution system incorporating DRM functions is schematically depicted in Fig. 1, which illustrates the relevant parties and their mutual relationships. The system typically includes a client having access to a network through an agreement, e.g. a subscription, with a network operator. This client-operator trust relation is usually manifested in a cryptographic relationship, i.e. sharing symmetric keys or having access to each other's public keys (certified by a commonly trusted party), if asymmetric cryptography is used. A trust relationship is also present between the network operator and the content provider, but in the form of a business agreement. This agreement could be manifested by a similar key sharing and/or key access as described for the client and network operator above. However, between the client and the content provider, an induced trust relationship is established each time the client obtains digital content from the content provider. This induced trust is manifested in a session key used for cryptographically protecting the digital content as it is transmitted to the client over the network.

In a typical content ordering and distribution process, the client firstly connects to the network operator. The operator then authenticates the client and possibly verifies that the client has a valid DRM agent for managing DRM metadata, such as usage rules, encrypted data and keys, associated with the digital content. The client chooses digital content or media and specifies some client-selectable usage rules to be valid for the media, for example rendering the media a selected number of times or during a given period of time. In the present description, digital content refers to digital data that can be downloaded or streamed over a network for usage in a client module, and thus includes for example audio, video, images, electronic books and other electronic text material as well as software (application programs, computer games, and so forth). Other types of usage of the digital content than rendering or execution includes forwarding, saving, copying and possibly modifying the digital content. In the following, the invention will mainly be described with reference to rendering of digital content. It should though be understood that the invention is not limited to rendering of audio, video and text, but

covers any usage or consumption of media content, including execution of application programs and computer games.

An order is then placed to the operator, which writes and encrypts a ticket specifying the ordered content and the usage rules. The ticket is sent to the client, where the DRM agent decrypts the ticket and extracts a session key from the received ticket. The ticket can be decrypted by conventional cryptographic means, e.g. using a key of a symmetric or asymmetric key pair associated with the client and the network operator. This decryption key is preferably the client-operator subscription key, a special DRM key associated with the DRM agent, or a key derived from these keys. The extracted session key will eventually be used for decrypting the digital media from the content provider. The client also receives a copy of the ticket encrypted with the operator-content provider agreement key (or a key derived therefrom). This ticket copy is forwarded to the content provider, where the session key is extracted after the validity of the ticket has been checked. Thereafter, the content provider delivers the ordered digital content cryptographically protected by the session key to the client, either as downloaded data or streaming data. Finally, a rendering or executing device in the client decrypts the digital content by the previously extracted session key. The digital content can now be used, e.g. rendered or executed, by the client or an associated device according to the usage rules. Further information regarding DRM systems and ordering and distribution of digital content can be found in [2], as well as in [3].

The overall content ordering and distribution process discussed above is merely given as a simplified example for conveying a general image of such processes. In order to increase the security, more authentication and cryptographic steps may be introduced. In addition, the client should pay for the ordered content, so billing and charging steps are most often present in the ordering process. Such a charging may be performed by a subscription to the network operator, by sending the client's credit card number to the network operator or a dedicated billing institute managing the charging of digital content, or by some other means. In addition, the network operator may provide both the network

and the digital content and hence acts as both operator and provider at the same time. However, the operator then typically has a dedicated content server and a dedicated operator server, so that the parties illustrated in Fig. 1 are present although the network operator also manages the content providing services. In some applications, e.g. WAP (Wireless Application Protocol) applications, it is also possible that another client may act as a content provider. The usage rules are then pushed to the content-receiving client from the network operator or the content provider.

It has been recognized that a partial solution to the objective problems addressed in the background section may be to use a portable tamper-resistant device that can be moved between rendering or executing devices. However, if a user buys a new device, there is typically some cumbersome set-up procedure before the new device can be used. In addition, it might even be that not at all combinations of DRM devices and rendering devices are interoperable.

The basic idea according to the invention is to implement a DRM agent in a network subscriber identity module that is intended for cooperation with a client module, such as a mobile phone or a computer system. The DRM agent is generally implemented with functionality for enabling usage, such as rendering or execution, of protected digital content provided to the client from a content provider. In general, the DRM agent includes functionality for cryptographic processing of DRM metadata associated with the digital content to be rendered. This metadata may for example be key(s) and user data such as the encrypted digital content itself. Normally, the DRM agent includes some basic functionality for more or less directly generating or extracting a decryption key to be used for decrypting the encrypted digital content. It is also possible to integrate the actual decryption of the digital content into the DRM agent, as well as functionality for rule-enforcement.

Due to the inherent tamper-resistance of the SIM, a proper security configuration will be hard to override. By implementing the DRM agent in an SIM, the agent is potentially

more secure than in a hostile PC environment. This is because the operating system platforms of PCs, e.g. Windows and Linux, are more well known by the public than corresponding platforms of SIM modules, which thereby become harder to attack and modify. The SIM is the base for a charging mechanism that can be used also for payment of digital content in the DRM system.

The fact that the SIM normally is removably arranged in relation to the client module makes it easy to move the SIM, with its DRM agent, between different devices, and also facilitates replacement of the DRM agent if it should be hacked.

Although the DRM agent may be implemented as special hardware in the network subscriber identity module, the currently most preferred implementation concerns a software-based DRM agent. It has been recognized that it is particularly advantageous to implement the DRM agent as an application in the application environment provided by the network subscriber identity module's application toolkit, such as the GSM SIM application toolkit (SAT) or the UMTS SAT (USAT). The DRM application agent can be preprogrammed into the toolkit application environment, or securely (preferably authenticated and encrypted) downloaded from a network operator associated with the subscriber identity module. The SAT provides an environment that can easily be upgraded with new software in a secure way, more of which below.

In addition, the mobile operator's infrastructure can be used to solve the set-up problems associated with using the DRM agent with new rendering devices, as will be explained later on.

Fig. 2A schematically illustrates a client module according a preferred embodiment of the present invention. The client or client module may be any form of appliance, which may order and obtain digital content over a network, for example a mobile phone with a SIM card removably arranged in a SIM card slot, or a personal computer equipped with a SIM card reader into which a SIM card is inserted. In this exemplary embodiment, the

client module comprises a network communication unit, a network subscriber identity module and a rendering (or executing) device. The network communication unit implements a network communication protocol stack, and thus enables downloading or streaming of digital content from a content provider to the client, using wireless or non-wireless network communication. The network subscriber identity module, hereinafter simply referred to as a subscriber identity module or a SIM, may be any SIM known to the art, including standard SIM cards used in GSM mobile telephones, as well as UMTS SIM cards, and WAP SIM and ISIM modules. The SIM could also be issued by a non-telecommunication actor, e.g. a smart card issued by a bank to its customers. As mentioned above, the SIM comprises a DRM agent implemented in hardware, software or a combination thereof. The rendering device could also be implemented in software, hardware or a combination thereof. Preferably, the rendering device includes a media processor, which may be software-implemented, for rendering the digital content using e.g. a screen or a loudspeaker, depending on the type of digital content. The rendering device usually comprises some form of DRM functionality, for example rule-enforcement and typically also decryption of the protected media content based on a key generated by the SIM-based DRM agent.

The rendering device may be integrated into the mobile unit or the PC, but can also be provided as a stand-alone device directly (via suitable communication ports) or indirectly connected thereto. In the latter case, the client may have one unit for downloading or streaming of digital content and another physically separate unit for actually rendering the digital content, i.e. the rendering device. The downloading or streaming unit may e.g. be a personal computer or mobile unit with suitable hardware/software for receiving the digital content. The protected digital content, together with a DRM-derived decryption key, may then be stored in or on some suitable portable media, including floppy disks, CD-ROM disks and DVD disks for transfer to an external rendering device for decryption and subsequent rendering. In practice, however, it may be more convenient to transmit the content to the rendering device via ordinary cables or by wireless

communication with or without involving a network. Typical stand-alone rendering devices include Mp3 players, CD players, DVD players, other mobile units or PCs.

As mentioned above, the DRM agent may preferably be implemented as a software application in the SIM, as schematically illustrated in Fig. 2B. The subscriber identity module preferably comprises an input/output unit, a resident subscription (GSM/UMTS/WAP) application, an AKA (Authentication and Key Agreement) module, a subscriber key k as well as an application environment. The I/O unit parses commands sent to the SIM and handles communication with the internal functions. The AKA module comprises algorithms for mutual authentication between client and network, and for deriving keys. This AKA function typically uses a SIM specific key, e.g. the subscription key k associated with the client-operator subscription, a key derived therefrom or a key x associated with the DRM agent implemented in the SIM. It is also possible to use asymmetric cryptography for authentication purposes. This function could for instance be the GSM A3/A8 AKA algorithms. The application environment is advantageously provided by the application toolkit of the subscriber identity module. For a GSM SIM the application environment may be provided by the SIM Application Toolkit (SAT) [4], whereas the analogue application environment of UMTS SIM (USIM) is provided by UMTS SAT (USAT) [5].

For a GSM SIM, the SIM-ME (SIM-Mobile Equipment) interface as defined in [6] specifies the "commands" and data that can be sent to/from the SIM/ME. For instance, to run the GSM A3/A8 AKA algorithms, there is a "RUN_GSM_ALGORITHMS"-command that computes the response and the ciphering key from a random challenge RAND and the stored subscriber key, k. In the list of commands possible over the SIM-ME interface, we specially note the "ENVELOPE" command, which is intended to send more or less arbitrary data to the SIM for use with the SIM Application Toolkit (SAT). The input/output format to the SIM is explicitly specified, but there is a high degree of freedom exactly what the applications can do or not. For instance, the application could be a quite general Java Applet, see [7]. The applet can be given

various degrees of authorization to access resident GSM-related files, one possibility being to give it "full GSM access".

In a preferred embodiment of the invention, the DRM agent is implemented in the application environment provided by the SIM application toolkit, using the "ENVELOPE" command or an analogous command. The SIM application toolkit thus enables the operator to "hardcode", or download, over the air in the case of a mobile, a DRM agent application into the SIM besides the default GSM/UMTS/WAP application. In the latter download case, it is also possible (and strongly recommended) to authenticate the DRM application as coming from the right operator. This is important since it gives protection against downloading "viruses" from malicious servers. The downloaded DRM application can also be encrypted so that the content of it is not available outside the SIM. For security aspects related to GSM SAT, reference is made to [8]. For communication between the DRM agent and the AKA module, there is preferably a direct interface between the AKA module and the SAT application environment.

By implementing the DRM agent of the SIM in the application environment, it is also possible to upgrade the functionality of the DRM agent. Upgradings are simply downloaded using download commands associated with the client module, e.g. using the ENVELOPE command, and implemented in the client module. This is an advantageous solution if the DRM agent is broken or "hacked", so that its code and/or secret keys become publicly available, e.g. on the Internet. Then, instead of changing all client modules, the associated DRM agent is simply updated by downloading and implementing new algorithms and or keys. On subsequent authentications, it can then be verified that the DRM agent is a compliant DRM agent of an allowed version.

For more information on fundamental details of the GSM SIM specification, reference is made to [9].

For encryption and authentication in the DRM system, any standard cryptographic techniques may be used, including both symmetric and asymmetric encryption and authentication. Using symmetric encryption and/or authentication, the encryption key is a shared symmetric key, a copy of which is stored both in the SIM and at the network operator or content provider. Alternatively, an asymmetric key pair may be used for encryption and authentication based on a Public Key Infrastructure (PKI). For asymmetric encryption, the public key is used for encryption and the corresponding private key for decryption. For asymmetric authentication, the private key is used for signing and the corresponding public key for verification. Also, subscription-associated usernames and passwords may be used in the context of authentication. If the client has one or several IP addresses associated thereto, such address(es) can also be used for authentication.

In the following, however, encryption and authentication will mainly be described in the context of symmetric cryptography, using the SIM subscriber key k and/or a DRM specific key x. The DRM specific key x, may be located anywhere in the SIM, preferably in the application environment, and even integrated in the DRM agent.

Fig. 3 is a flow diagram illustrating a digital rights management method according to a preferred embodiment of the invention. The method is directed towards the network operator side of the overall DRM system, and concerns the downloading of a DRM agent into a SIM arranged in relation to a client module. As a recommended, but optional first step (S1) mutual authentication is performed between client and operator. The operator may optionally generate authentication data for transmission to the SIM module of the client to enable the client to authenticate that the DRM agent comes from a trusted operator. The operator performs a download (S2), optionally authenticated, of a DRM agent into the SIM, preferably as an SAT application using the "ENVELOPE" command. If required, for example due to a security flaw, the DRM agent may be remotely upgraded (S3) by the network operator, which downloads the required patches or entirely new DRM algorithms. The operator or content provider may also

authenticate that requesting clients have SIM modules with compliant DRM agents, using any known authentication technique. This authentication of the DRM agent normally includes verification that the DRM agent is of a compliant type, but preferably also includes DRM agent version verification.

Fig. 4 is a schematic diagram illustrating an example of client-operator authentication key agreement client-side digital rights management, as well as the associated client-operator communication. In this particular example, the client sends an authentication tag, which preferably is dependent on some secret key such as a symmetric key shared by the SIM module and the operator, or a private key. In the case of symmetric authentication, which is assumed here, it is possible to use the subscriber key k and/or a special DRM key x. The operator performs authentication key agreement (AKA) using a random challenge, rand, other optional user data, the key k and or the key x as input to a cryptographic function f, thus generating a session key t to be used for secure communication between the client and the operator. The operator sends the rand value, possibly together with an authentication tag, to the SIM module of the client. The data is received by the client's SIM module and, if an authentication tag is present, the SIM module first authenticates the received data and then runs the same AKA function f with the same input to derive the session key t and a response, res. The response is sent back to the operator so that it can be verified that the operator is in contact with the right application. In the following, $E_z(m)$ represents a message m, protected by a key z. "E" is intended to denote "encryption", but it may (and often should) also encompass authentication and integrity protection. Next, the client places an order, protected by the session key t, to the operator. The operator, which acts as an order server, generates a ticket and a further session key s, also referred to as a media protection key, and encrypts the ticket and the key s with the previously generated session key t. The encrypted ticket and media protection key s is sent to the client, which invokes the DRM agent in order to decrypt the ticket and the media protection key s by using the key t. The media protection key s together with the associated ticket is also securely forwarded to the content provider, which then encrypts the ordered

digital content by using the media protection key s and sends the protected media to the client. Once received by the client, the protected media content is decrypted, either by the DRM agent or more likely by some DRM functionality present in the rendering device, using the media protection key s.

As previously indicated, the DRM agent implemented in the SIM basically includes functionality for cryptographic processing of DRM metadata associated with the digital content to be rendered. This metadata may for example be one or several keys as well as encrypted information. Normally, the DRM agent includes some basic functionality for more or less directly generating or extracting a decryption key to be used for decrypting the encrypted digital content, as described below with reference to Fig. 5.

Fig. 5 illustrates a subscriber identity module and an associated rendering device according to an embodiment of the invention. The block diagram of Fig. 5 only illustrates those components that are relevant to the invention. The SIM module has an AKA module, and a DRM agent. Among other things, the AKA module generates the session key t, preferably based on the subscriber key, k, and/or a special DRM key, x. The DRM agent comprises a cryptographic unit C1 for extracting the media protection key (also referred to as a session key) s based on the session key t received from the AKA module and the encrypted information $E_t(s)$ received from the network operator. In this embodiment, the actual decryption of the media content takes place in the rendering device, which is integrated in the same module as the SIM or provided as an external stand-alone device directly or indirectly connected to the mobile, PC or other equipment in relation to which the SIM is arranged. The rendering device includes a DRM module, which in turn has a cryptographic unit C2 for decrypting the protected media content from the content provider by using the media protection key extracted by the DRM agent in the SIM module. The decrypted media content is finally sent to a media processor in the rendering device for preparing the actual rendering.

If the actual rendering/decryption is done in another tamper-resistant module, distinct from the SIM, it might be advisable to configure that device and the SIM DRM application by a shared secret key, y, so that the media protection key s can be sent encrypted between the SIM and that device, as illustrated in Fig. 6. Now, the DRM agent in the SIM comprises two logically separated (in practice, though, they may be implemented in one and the same hardware/software module) cryptographic units C1 and C3. The cryptographic unit C1 is similar to that of Fig. 5, whereas the cryptographic unit C3 is configured to encrypt the protection key s by using the key y, before transmittal to the rendering device. The DRM module in the rendering device now includes a cryptographic unit C4 for decrypting the encrypted key s by using the key y, and a cryptographic unit C2 for decrypting the media content by using the decrypted key s.

This also enables the SIM application to authenticate that it is in contact with such a tamper resistant device. The SIM could either rely on implicit authentication, i.e. only a device knowing the key y can decrypt the key s, or perform an explicit authentication based on the key y. If the rendering device is a stand-alone device, it is recommended that it has its own rule-enforcement and is given the usage rules in the ticket along with the media so that it can act as an agent on behalf of the content owner/provider and assert that the usage rules are followed. Otherwise, for example in a mobile unit with its own rendering application, the rule enforcement could alternatively be implemented directly in the DRM agent.

As the key y is specific to the rendering device, the client (SIM) may establish a trust relation with that device, in particular the very first time when the device is brand new. Note that it is not secure to simply write "y" on the outside of the device, as it could be copied and a cloned, and a non-secure device could easily be created. Instead, the result of applying some cryptographic one-way function h to the key y may be attached to a "label" on the rendering device when it is sold. Each device is associated with a random, secret y-value, and when the buyer wishes to activate the device, he

sends h(y) to the operator (or another trusted certification party) who checks that h(y) is assigned to a valid device and updates the DRM application in the SIM with the key y. It is assumed that the operator has some secret key that enables him, and no one else, except possibly the device manufacturer to invert the function h. The value y can be checked to verify that only "authentic" (i.e. not stolen, hacked or otherwise compromised) rendering devices, ones with "valid" y-values, are used in the system, and if a user purchases a new rendering device, he can add support (a new key in his SIM) for it in a simple way. This can be used for certification and registration, in said subscriber identity module, of various rendering devices with which the client (SIM) wants to establish trust relations.

It should though be understood that the response of sending the "labeled" identification key to the certification party may be any a representation of the rendering device key y allowing the DRM agent to derive the key y.

Due to the limited processing capacity of the SIM modules of today, it is normally recommendable to perform the actual decryption of the digital content in the rendering device. However, with increased processing capacity in the SIM, it is equally feasible to integrate the decryption of the content into the DRM agent, as illustrated in Fig. 7. Here, the SIM comprises both the cryptographic unit C1 for generating the media protection key s, and the cryptographic unit C2 for decrypting the encrypted media content using the protection key s from the cryptographic unit C1. The decrypted media content is then sent to the rendering device for processing and rendering.

For a more complete understanding, an exemplary SAT-based solution will now be described with reference to Figs. 8 and 9, which schematically illustrate the overall DRM protocol and the corresponding block diagram, respectively.

As mentioned, in a DRM solution, part of the processing normally must take place in a tamper resistant device, preferably a SIM. Typically, a container is downloaded that

comprises key(s) and/or data, and this key(s)/data need to be processed in a protected environment. Here, the processing behavior could be entirely specified by a SAT application, possibly interfacing with the authentication/key generation algorithms pre-existing on the card, reusing the operator-subscriber relation. Using SAT in this context is not the same as using a "true" tamper resistant module, but it is more secure than performing the processing in a hostile PC environment and more flexible than using hard-wired tamper resistant modules. If a security flaw is found, the card is easily upgraded (even over the air) by a new set of DRM processing algorithms.

In this example, it is assumed that the SIM card contains k, the usual subscriber key. The SIM also contains an application environment (e.g. SAT/USAT) that is premanufactured with a DRM application, or alternatively, the DRM application is securely (encrypted and authenticated) downloaded. Also, a second key, x, specific for DRM purposes is present in the SIM and at the operator. Like k, also x is stored so that it cannot be read out of the SIM card. Note though that x may be stored in software, e.g. as part of the DRM application, if enough protection can be guaranteed. Besides the network operator, there is a content provider, which, if distinct from the operator, has a contractual agreement with the operator, manifested by a shared key c.

First, and optionally, each time the DRM agent in the SIM is to be invoked, the application verifies that it is running in a trusted environment, e.g. by a mutual authentication protocol. This protocol could be based on knowledge of the key x, or some other information shared between the SIM and the device with which the SIM is related, e.g. another key y. This might be desirable in cases where the whole SIM can be moved between devices, in which case there is one unique key, y, for each device the SIM is used with. Such solutions are (partly) already available in mobile phones, in order to lock the SIM to a specific mobile (so called SIM-lock feature).

When the user has decided what media he wants (and possibly paid for it, if payment is not done afterwards or during the session), he notifies the network operator that he wishes to use the DRM application, and the operator performs authentication and key-

agreement using a random challenge rand, other optional user data, the key x and optionally also the key k. This authentication could optionally have been done before, e.g. when gaining network access. The key k is used when it is necessary or appropriate to tie the key generation to the subscription as such. This AKA is done using some cryptographic function f, which, in case we desire dependence also on k, may partially consist of the normal SIM authentication algorithm.

In other words, the operator sends rand (and optional [user_data], if not already known by the DRM application on the SIM) to the SIM (see (1) in Fig. 9). The information sent is preferably authenticated, e.g. by a key derived from k and/or x in a similar way. The data is received by the DRM application on the SIM, which, if an authentication tag is present, first authenticates the received data, and then runs the same function f to derive the session key, t and the response, res. This response is sent back to the operator so that the operator can verify that it is in contact with the right application. Subsequently, the application places an order (protected by the key t) on what media and what rights it wishes to gain to the operator. The order is typically generated by a browser application in the device, which passes it to the AKA module or DRM application for encryption (note that the browser application is in this case also a trusted and authenticated application, or the user must be given the possibility to confirm the placed order). The operator returns a session key s, along with a ticket describing the ordered media and rights. This session key is to be later used for the actual media protection. The ticket and the session key s are sent in duplicates. One is protected by the key c (known only to the content provider and the operator), the other is protected by the key t (known only to the client and the operator). The client decrypts the ticket and the key s and checks that the ticket corresponds to the earlier placed order.

The key s can now be output to another application in the device (not necessarily on the SIM itself), or, to a completely stand-alone external device, that using the key s later decrypts the received media and renders it to the user. Note that it may be the

case that the actual rendering/decryption is done in another tamper-resistant module, distinct from the SIM. If so, as mentioned above, it might be advisable to configure that device and the SIM DRM application by a shared secret key, y, so that s can be sent encrypted between the SIM and that device (see (2) in Fig. 9). This also, as discussed above, enables the SIM application to authenticate that it is in contact with such a tamper resistant device. The SIM could either rely on implicit authentication (i.e. only a device knowing the key y can decrypt the session key s), or perform an explicit authentication based on the key y. If the rendering device is "stand-alone" it is recommended that it has its own rule-enforcement and is given the usage rules in the ticket along with the media so that it can act as an agent on behalf of the content owner/provider and assert that the usage rules are followed. The rule enforcement could alternatively be implemented in the SIM, or distributed between the SIM and the rendering device.

The client next sends the ticket and session key s (still protected by the key c) to the content provider (see (3) in Fig. 9). The content provider removes the protection from the ticket and extracts the key s. If this is successful, the content provider knows that the ticket originated from an operator with whom he has an agreement. If any set-up messages are needed between the client and the content provider prior to sending the media, this traffic is protected by the key s (or some other key derived from s). Finally, the content provider encrypts the media by the session key s, and sends (downloads or streams) it to the rendering device (see (4) in Fig. 9).

It is also possible to let the rendering device authenticate that the media protection key s really comes from a SIM that has been paired with the rendering device through the shared secret key, y.

Note that if the rendering device is to be transferred to another user, having another DRM agent, it is normally recommended that the "y" in the rendering device be upgraded, so that the old DRM agent cannot be used with it anymore. This could be

done by an authorized service point, or remotely over a network. On the other hand, there could also be cases when it is desired that the same device can be used by two (or more) different DRM agents.

It is also recognized that the use of "keys" inside devices could be used for anti-theft purposes: without knowing the key, the device is useless, and if someone tries to configure a device, it could be checked against a register of stolen devices.

The ticket-based protocol above is of course not the only possible; many variations exist as can easily be seen by those of ordinary skill in the art.

The invention fits well into the emerging WAP-DRM standard. The Wireless Application Protocol (WAP) is standardized by WAP-Forum. There is currently ongoing work to come up with a way to enforce DRM in the scope of WAP [10, 11]. At present, the standardization work is mainly targeted at download.

The WAP solution separates the media download of a DRM object in two parts: the media object and the rights object. The download can be performed using one of three defined methods:

- Forward-lock: The client downloads only the media object. The media object has some simple default rights, e.g. a "preview object", and can not be forwarded to another user.

- Combined download: The client downloads both the media object and the rights object.

- Separate delivery: The client downloads the media object, which is encrypted with a key CEK (Content Encryption Key). The rights object can later (or simultaneously) be pushed to the client.

The client is assumed to be an authorized entity, i.e. the device in which it resides can trust that the client behaves in a good way, and obeys any rights imposed by a rights object. No non-authorized entity, e.g. a text-editor or a game that is installed in the device has access to the DRM objects in unencrypted form (possibly not even in encrypted form).

The WAP DRM client defined in [10, 11] can suitably be implemented as an SAT application in an SIM-card as described above. The WAP-DRM standard however, assumes that the media rendering device and the download client both resides in the same physical entity. This limitation can be relaxed without violating the WAP-DRM standard by configuring the rending device and the SIM DRM application by a shared secret key, y, so that the CEK key can be sent in protected form between the SIM and the rendering device.

The Forward-lock and Combined download models specify that the media and rights are downloaded to the DRM client. According to the invention, the rights object may be included in the ticket, and the media object may be downloaded to the rendering device. Note that in this respect there is no real difference between download and streaming. In references [10, 11] that are mainly targeted at download, there is a suggestion to perform streaming by downloading an SDP description of the stream in the media object, and then use that description to set up the streaming session. It poses no problems at all to fit that into the solution proposed by the invention, the SDP description is simply passed inside the ticket. For information on SDP, reference is made to [12]. Preferably, the DRM client implemented in the application environment of the SIM also includes functionality for checking that the forward-lock function of the WAP Protocol is not violated.

The Separate delivery model specifies a way to first download the media object, and then separately download, or rather push, the rights object to the client. The invention can be used also in the implementation of this model. The media object is protected by

a Content Encryption Key (CEK). With the notation used in the protocol of the invention, the media protection key s is an instantiation of the CEK. The invention also provides a way to authenticate the download client to the device and vice versa, e.g. based on the key x. This authentication is left as "out of scope" in [10, 11].

The embodiments described above are merely given as examples, and it should be understood that the present invention is not limited thereto. Further modifications, changes and improvements which retain the basic underlying principles disclosed and claimed herein are within the scope and spirit of the invention.

REFERENCES

[1] A. J. Menezes, P.C. van Oorschot and S.C. Vanstone, "Handbook of Applied Cryptography", CRC Press.

[2] L. Kaati, "Cryptographic Techniques and Encodings for Digital Rights Management", Master's Thesis in Computer Science, Department of Numerical Analysis and Computer Science, Royal Institute of Technology, Stockholm University, 2001.

[3] Swedish Patent Application No. 0101295-4 filed April 10, 2001.

[4] "Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface", 3GGP TS 11.14, ETSI TS 101 267, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, Version 8.10.0, 1999.

[5] "USIM Application Toolkit (USAT)", 3GGP TS 31.111, ETSI TS 131 111, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, Version 4.4.0, Release 4.

[6] "Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface" 3GPP TS 11.11, ETSI TS 100 977, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, Version 8.5.0, 1999.

[7] "GSM API for SIM Toolkit, Stage 2", 3GGP TS 03.19, ETSI TS 101 476, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, Version 8.4.0, 1999.

[8] "Security Mechanism for SIM Application Toolkit, Stage 2", 3GGP TS 03.48, ETSI TS 101 181, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, Version 8.8.0, 1999.

[9] "Subscriber Identity Modules (SIM), Functional Characteristics", ETSI TS 100 922, GSM 02.17, Technical Specification Digital Cellular Telecommunications system, Version 3.2.0, February 1992.

[10] "Download Architecture Version 1.0", Proposed version 10-June-2002, Open Mobile Alliance.

[11] "Digital Rights Management Version 1.0", Proposed version 28-June-2002, Open Mobile Alliance.

[12] M. Handley, V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998.

CLAIMS

1. A network subscriber identity module adapted for cooperation with a client module capable of receiving digital content provided from a content provider over a network,

wherein said network subscriber identity module comprises a digital rights management (DRM) agent for enabling usage of said digital content.

2. The network subscriber identity module according to claim 1, wherein said DRM agent is implemented as an application in the application environment provided by an application toolkit associated with said network subscriber identity module.

3. The network subscriber identity module according to claim 2, wherein said DRM agent application is downloaded into said network subscriber identity module from a network operator associated with said network subscriber identity module.

4. The network subscriber identity module according to claim 3, wherein said DRM agent application is remotely upgradeable.

5. The network subscriber identity module according to claim 3, wherein said network subscriber identity module includes means for authenticating that said DRM agent application comes from said network operator.

6. The network subscriber identity module according to claim 5, wherein said network subscriber identity module and said associated network operator share a common key, and said authenticating means is operable for authenticating said DRM agent application based on said common key.

7. The network subscriber identity module according to claim 6, wherein said common key is a subscriber key of said network subscriber identity module.

8. The network subscriber identity module according to claim 1, wherein said DRM agent includes functionality for cryptographic processing of DRM metadata associated with said digital content.

9. The network subscriber identity module according to claim 1, wherein said DRM agent implemented in said network subscriber identity module includes functionality for generating a decryption key that is to be used for decrypting encrypted digital content provided from said content provider.

10. The network subscriber identity module according to claim 9, wherein said network subscriber identity module and an associated network operator share a common key, and said decryption key generating functionality is operable for generating said decryption key at least partly based on said common key.

11. The network subscriber identity module according to claim 10, wherein said common key is a subscriber key of said network subscriber identity module.

12. The network subscriber identity module according to claim 10, wherein said common key is a special DRM key stored in said network subscriber identity module.

13. The network subscriber identity module according to claim 12, wherein said DRM agent is implemented as an application in the application environment provided by an application toolkit associated with said network subscriber identity module, and said special DRM key is also stored in said application environment.

14. The network subscriber identity module according to claim 9, wherein said DRM agent implemented in said network subscriber identity module further includes functionality for decrypting said encrypted digital content by means of said generated decryption key.

15. The network subscriber identity module according to claim 1, wherein said DRM agent implemented in said network subscriber identity module includes functionality for enforcement of usage rules associated with said digital content.

16. The network subscriber identity module according to claim 1, wherein said DRM agent implemented in said network subscriber identity module includes functionality for certification and registration, in said network subscriber identity module, of a rendering or executing device.

17. The network subscriber identity module according to claim 1, wherein said DRM agent implemented in said network subscriber identity module includes functionality for checking that the forward-lock function of the Wireless Application Protocol (WAP) is not violated.

18. A network subscriber identity module comprising digital rights management functionality.

19. A client module comprising:

- means for receiving digital content provided from a content provider over a network; and
- a network subscriber identity module implemented with a digital rights management (DRM) agent for enabling usage of said digital content.

20. The client module according to claim 19, wherein said DRM agent is implemented as an application in the application environment provided by an application toolkit associated with said network subscriber identity module.

21. The client module according to claim 20, wherein said DRM agent application is downloaded into said network subscriber identity module from a network operator associated with said network subscriber identity module.

22. The client module according to claim 21, wherein said DRM agent application is remotely upgradeable.

23. The client module according to claim 21, wherein said network subscriber identity module includes means for authenticating that said DRM agent application comes from said network operator.

24. The client module according to claim 23, wherein said network subscriber identity module and said associated network operator share a common key, and said authenticating means is operable for authenticating said DRM agent application based on said common key.

25. The client module according to claim 24, wherein said common key is a subscriber key of said network subscriber identity module.

26. The client module according to claim 19, wherein said network subscriber identity module is removably arranged in relation to said client module.

27. The client module according to claim 19, wherein said DRM agent includes functionality for cryptographic processing of DRM metadata associated with said digital content.

28. The client module according to claim 19, wherein said DRM agent implemented in said network subscriber identity module includes functionality for generating a decryption key to be used for decrypting encrypted digital content provided from said content provider.

29. The client module according to claim 28, wherein said network subscriber identity module and an associated network operator share a common key, and said

decryption key generating functionality is operable for generating said decryption key at least partly based on said common key.

30. The client module according to claim 29, wherein said common key is a subscriber key of said network subscriber identity module.

31. The client module according to claim 29, wherein said common key is a special DRM key stored in said network subscriber identity module.

32. The client module according to claim 31, wherein said DRM agent is implemented as an application in the application environment provided by an application toolkit associated with said network subscriber identity module, and said special DRM key is also stored in said application environment.

33. The client module according to claim 28, wherein said DRM agent implemented in said network subscriber identity module further includes functionality for decrypting said encrypted digital content by means of said generated decryption key.

34. The client module according to claim 19, wherein said DRM agent implemented in said network subscriber identity module includes functionality for certification and registration, in said network subscriber identity module, of a rendering or executing device.

35. The client module according to claim 34, wherein said client module includes means for transmitting, to a trusted certification party, an identification key of a rendering or executing device to be registered, and in response thereto, receiving a representation of a device key, and wherein said DRM agent in said network subscriber identity module includes means deriving, based on said reprcsentation, said device key for storage in said network subscriber identity module.

36. The client module according to claim 35, wherein said DRM agent includes:

- functionality for generating a decryption key to be used for decrypting encrypted digital content provided from a content provider; and
- functionality for encrypting the digital-content decryption key by said device key and for transferring said encrypted digital-content decryption key to said rendering or executing device.

37. The client module according to claim 19, wherein said DRM agent implemented in said network subscriber identity module includes functionality for checking that the forward-lock function of the Wireless Application Protocol (WAP) is not violated.

38. The client module according to claim 19, further comprising a rendering or executing device for rendering or executing said digital content.

39. The client module according to claim 38, wherein said DRM agent and/or said rendering or executing device includes functionality for enforcement of usage rules associated with said digital content.

40. A client-server based digital rights management (DRM) system, wherein the client module comprises:

- means for receiving digital content provided from a content provider over a network; and
- a network subscriber identity module implemented with a digital rights management (DRM) agent for enabling usage of said digital content.

41. The DRM system according to claim 40, wherein said DRM agent is implemented as an application in the application environment provided by an application toolkit associated with said network subscriber identity module.

42. The DRM system according to claim 41, wherein said DRM agent application is downloaded into said network subscriber identity module from a network operator associated with said network subscriber identity module.

43. The DRM system according to claim 42, wherein said DRM agent application is remotely upgradeable.

44. The DRM system according to claim 42, wherein said network subscriber identity module includes means for authenticating that said DRM agent application comes from said network operator.

45. The DRM system according to claim 44, wherein said network subscriber identity module and said associated network operator share a common key, and said authenticating means is operable for authenticating said DRM agent application based on said common key.

46. The DRM system according to claim 45, wherein said common key is a subscriber key of said network subscriber identity module.

47. The DRM system according to claim 40, wherein said network subscriber identity module is removably arranged in relation to said client module.

48. The DRM system according to claim 40, wherein a network operator/ content provider comprises means for authenticating that said network subscriber identity module comprises a compliant DRM agent.

49. The DRM system according to claim 40, wherein said DRM agent includes functionality for cryptographic processing of DRM metadata associated with said digital content.

50. The DRM system according to claim 40, wherein said DRM agent implemented in said network subscriber identity module includes functionality for generating a decryption key that can be used for decrypting encrypted digital content provided from said content provider.

51. The DRM system according to claim 50, wherein said network subscriber identity module and an associated network operator share a common key, and said decryption key generating functionality is operable for generating said decryption key at least partly based on said common key.

52. The DRM system according to claim 51, wherein said common key is a subscriber key of said network subscriber identity module.

53. The DRM system according to claim 51, wherein said common key is a special DRM key stored in said network subscriber identity module.

54. The DRM system according to claim 53, wherein said DRM agent is implemented as an application in the application environment provided by an application toolkit associated with said network subscriber identity module, and said special DRM key is also stored in said application environment.

55. The DRM system according to claim 50, wherein said DRM agent implemented in said network subscriber identity module further includes functionality for decrypting said encrypted digital content by means of said generated decryption key.

56. The DRM system according to claim 40, wherein said DRM agent implemented in said network subscriber identity module includes functionality for certification and registration, in said network subscriber identity module, of a rendering or executing device.

57. The DRM system according to claim 56, wherein said client module includes means for transmitting, to a trusted certification party, an identification key of a rendering or executing device to be registered, and in response thereto, receiving a representation of a device key, and wherein said DRM agent in said network subscriber identity module includes means for deriving, based on said representation, said device key, and means for storing said device key in said network subscriber identity module.

58. The DRM system according to claim 57, wherein said DRM agent includes:

- functionality for generating a decryption key to be used for decrypting encrypted digital content provided from a content provider; and
- functionality for encrypting the digital-content decryption key by said device key and for transferring said encrypted digital-content decryption key to said rendering or executing device.

59. The DRM system according to claim 40, wherein said DRM agent implemented in said network subscriber identity module includes functionality for checking that the forward-lock function of the Wireless Application Protocol (WAP) is not violated.

60. The DRM system according to claim 40, wherein said client module further comprises a rendering or executing device for rendering or executing said digital content.

61. The DRM system according to claim 60, wherein said DRM agent and/or said rendering or executing device includes functionality for enforcement of usage rules associated with said digital content.

62. A digital rights management (DRM) method comprising the step of:

- a network operator downloading, over a network, a DRM agent into a network subscriber identity module arranged in relation to a client module.

63. The DRM method according to claim 62, wherein said DRM agent is downloaded as an application into the application environment provided by an application toolkit associated with said network subscriber identity module.

64. The DRM method according to claim 62, further comprising the step of said network operator generating authentication data for transmission to said network subscriber identity module, thus enabling authentication that said DRM agent comes from said operator.

65. The DRM method according to claim 64, wherein said network subscriber identity module and said network operator share a common key, and said authentication data is generated based on said common key.

66. The DRM method according to claim 65, wherein said common key is a subscriber key of said network subscriber identity module.

67. The DRM method according to claim 62, wherein said DRM agent is remotely upgraded by said network operator.

68. The DRM method according to claim 62, further comprising the step of a network operator/content provider authenticating that said network subscriber identity module comprises a compliant DRM agent.

69. The DRM method according to claim 62, wherein said DRM agent is implemented with functionality for enabling usage of digital content in said client module.

70. The DRM method according to claim 69, wherein said DRM agent is implemented with functionality for cryptographic processing of DRM metadata associated with said digital content.

71. A client module comprising:

- means for receiving digital content provided from a content provider over a network; and
- a network subscriber identity module implemented with a digital rights management (DRM) agent, said DRM agent including:
  - functionality for generating a decryption key to be used for decrypting encrypted digital content provided from a content provider; and
  - functionality for encrypting the digital-content decryption key by a specific device key and for transferring said encrypted digital-content decryption key to a rendering or executing device.

72. The client module according to claim 71, wherein said DRM agent includes means for authenticating that it is in contact with a certified tamper resistant rendering or executing device based on said specific device key.

ABSTRACT OF THE DISCLOSURE

The invention relates to digital rights management, and proposes the implementation of a DRM agent into a network subscriber identity module intended for cooperation with a client module, such as a mobile phone or a computer system. The DRM agent is generally implemented with functionality for enabling usage, such as rendering or execution, of protected digital content provided to the client from a content provider. In general, the DRM agent includes functionality for cryptographic processing of DRM metadata associated with the digital content to be rendered. In a particularly advantageous realization, the DRM agent is implemented as an application in the application environment provided by the network subscriber identity module's application toolkit. The DRM application agent can be preprogrammed into the toolkit application environment, or securely (preferably authenticated and encrypted) downloaded from a network operator associated with the subscriber identity module.

(Fig. 2)

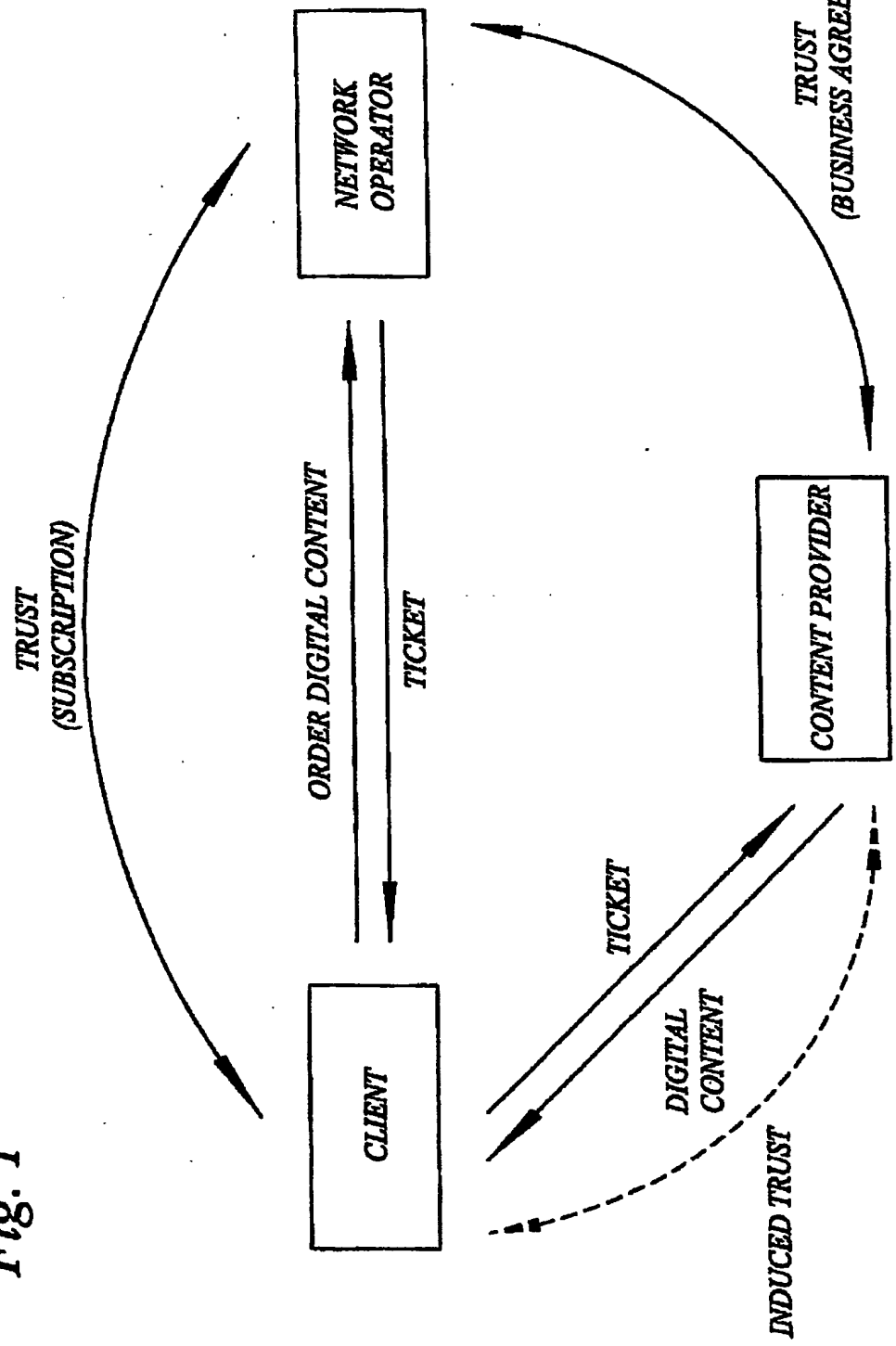

Fig. 1

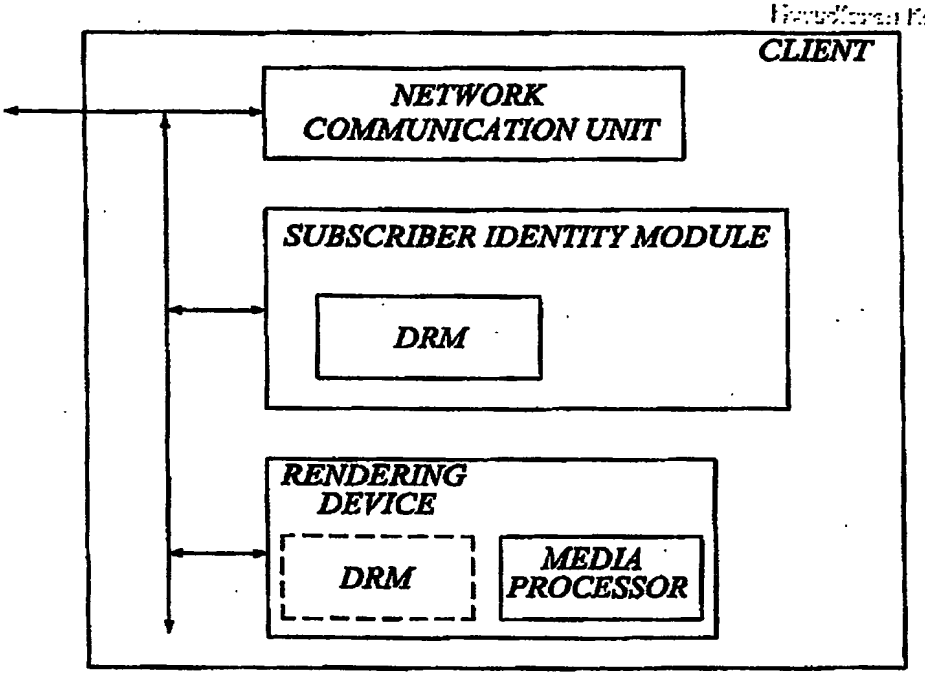

Fig. 2A

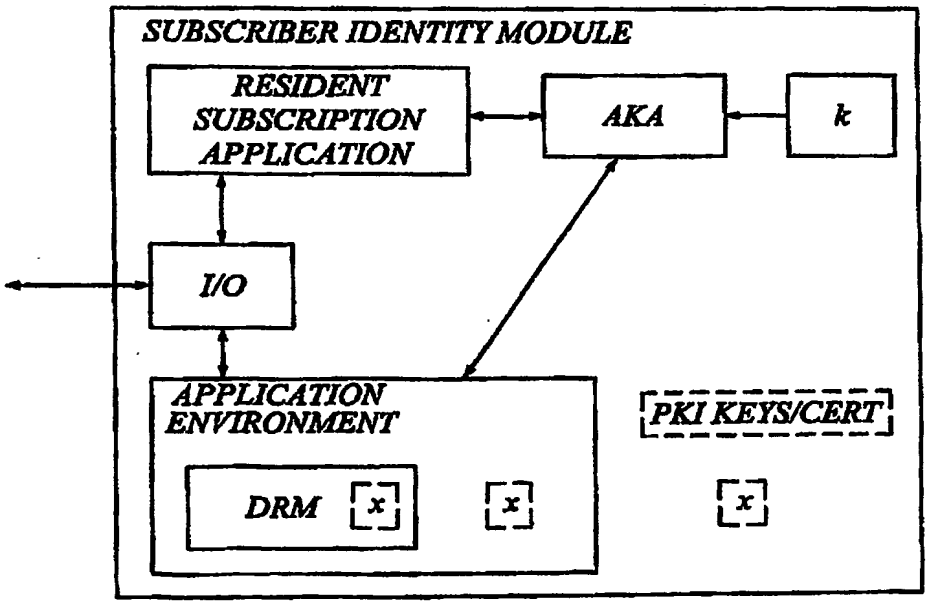

Fig. 2B

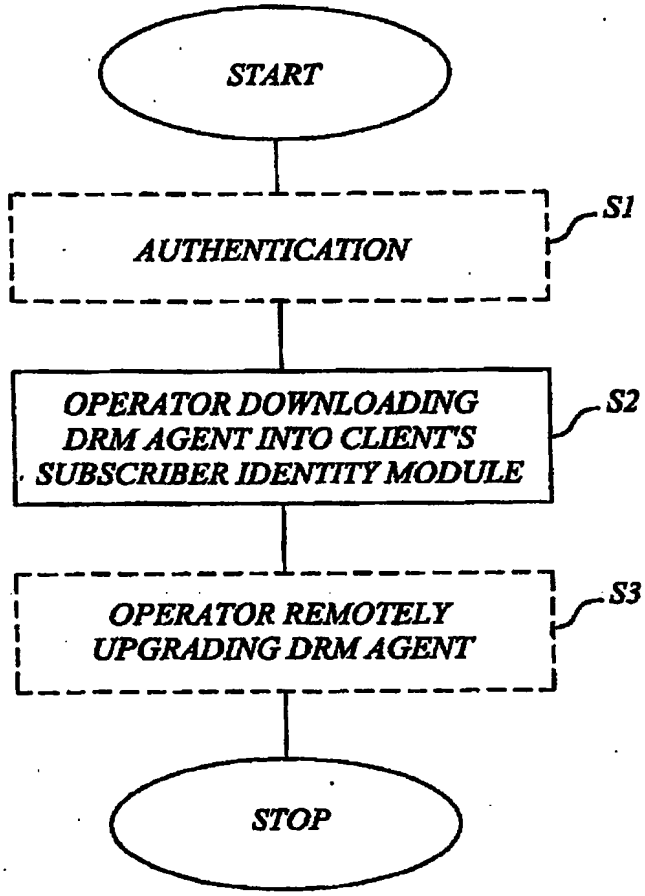
START
AUTHENTICATION
S1
OPERATOR DOWNLOADING DRM AGENT INTO CLIENT'S SUBSCRIBER IDENTITY MODULE
S2
OPERATOR REMOTELY UPGRADING DRM AGENT
S3
STOP

Fig. 3

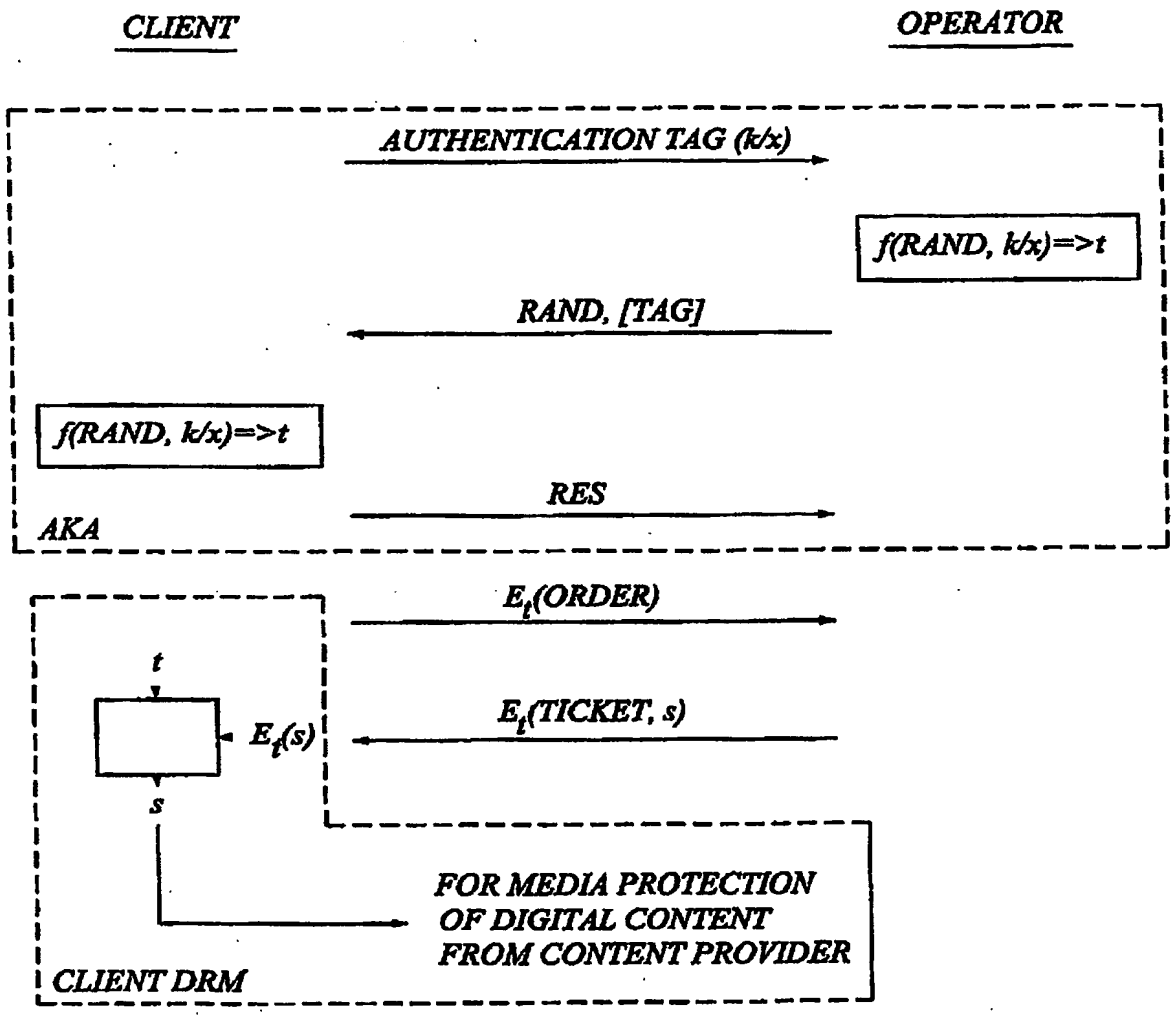
CLIENT
OPERATOR
AUTHENTICATION TAG (k/x)
f(RAND, k/x)=>t
RAND, [TAG]
f(RAND, k/x)=>t
RES
AKA
E_t(ORDER)
t
E_t(s)
E_t(TICKET, s)
s
FOR MEDIA PROTECTION
OF DIGITAL CONTENT
FROM CONTENT PROVIDER
CLIENT DRM

Fig. 4

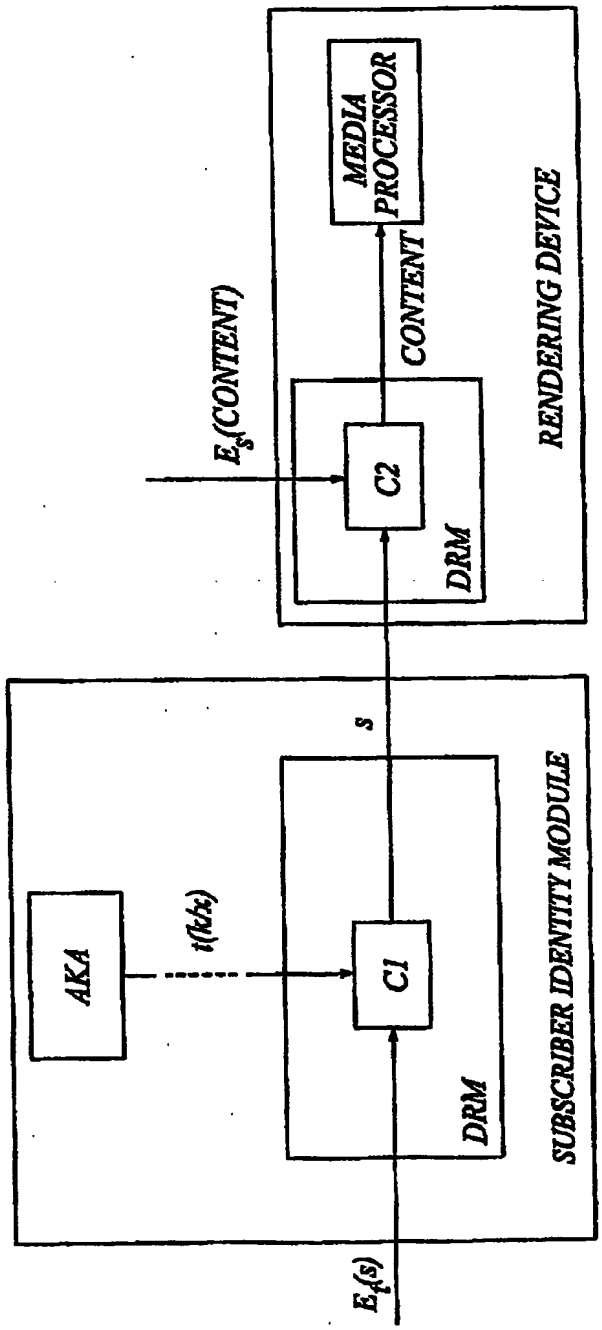

Fig. 5

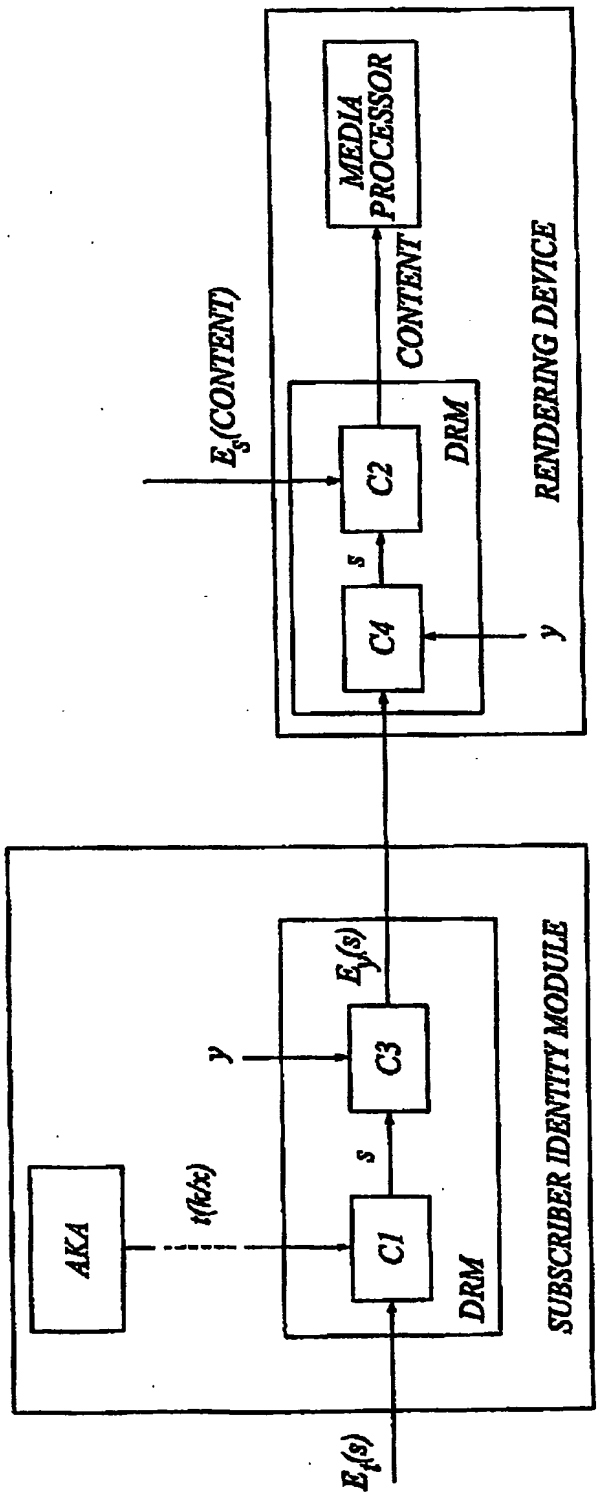

Fig. 6

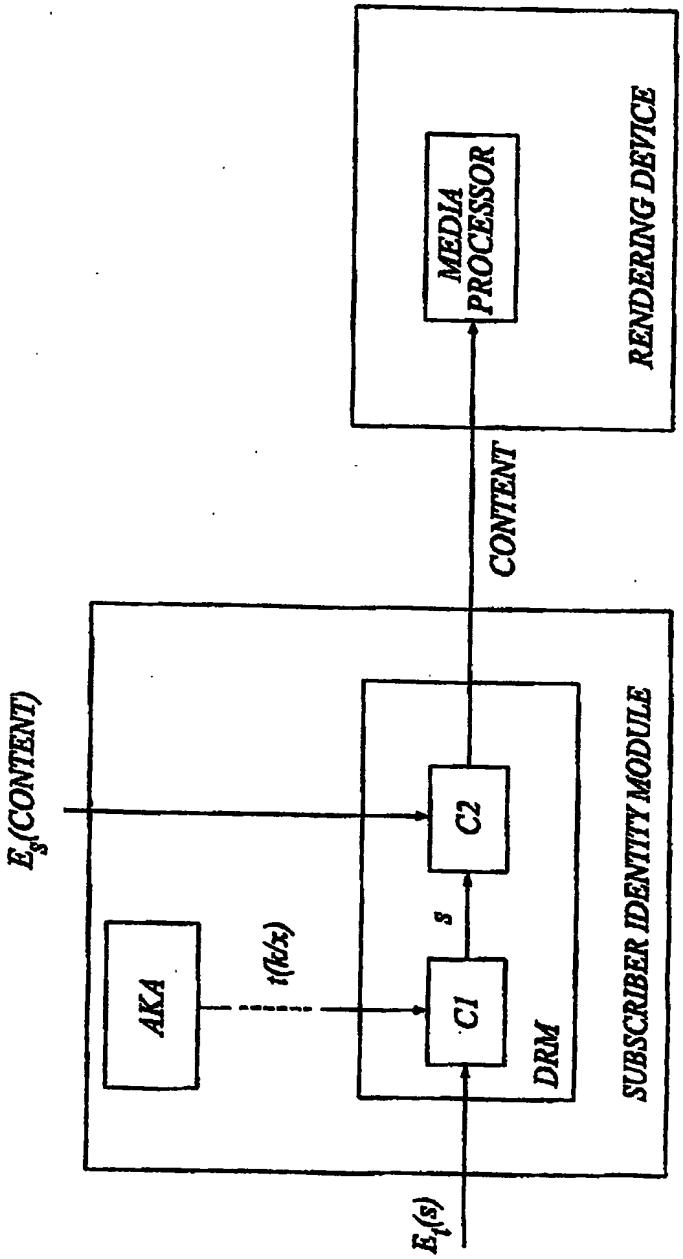

Fig. 7

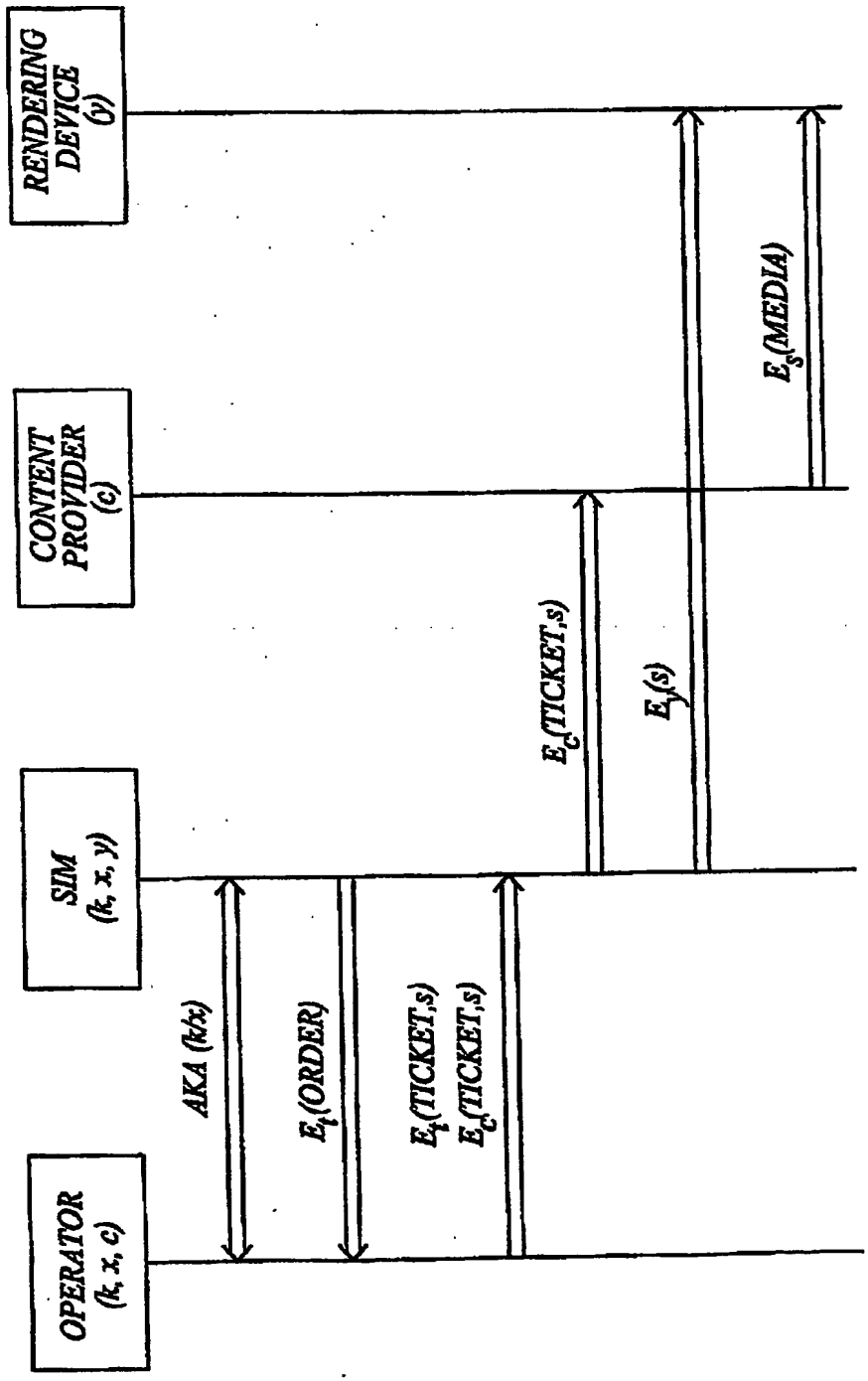

Fig. 8

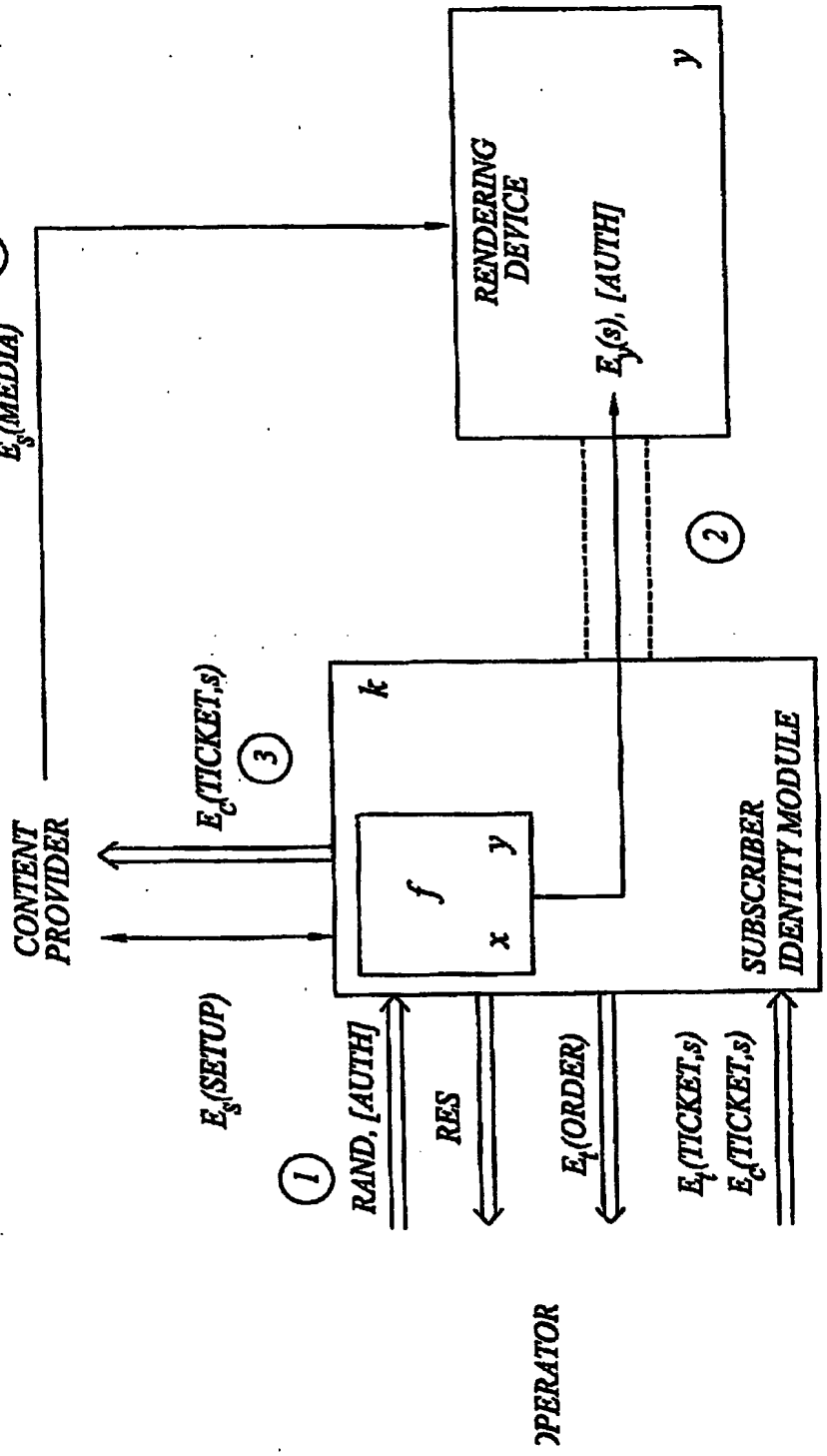
RENDERING DEVICE
y
$E_y(s)$, [AUTH]
4
E_s(MEDIA)
2
CONTENT PROVIDER
E_c(TICKET,s)
3
k
f
y
x
SUBSCRIBER IDENTITY MODULE
E_s(SETUP)
1
RAND, [AUTH]
RES
E_i(ORDER)
E_i(TICKET,s)
E_c(TICKET,s)
OPERATOR

Fig. 9

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.